PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-151574
(43)Date of publication of application : 30.05.2000

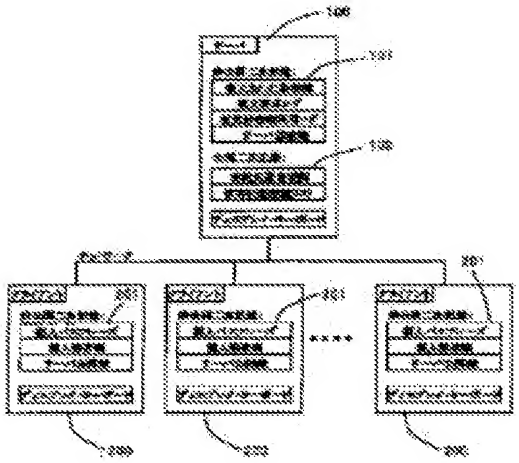
(51)Int.Cl. H04L 9/08
G06F 13/00
G09C 1/00

(21)Application number : 10-321867
(22)Date of filing : 12.11.1998

(71)Applicant : FUJI XEROX CO LTD
(72)Inventor : AOKI RYUICHI

(54) ENCRYPTION KEY DEPOSIT DEVICE AND METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To deposit an encryption key regularly and also sufficiently maintain security of the deposited encryption key by providing a scheme controlling the deposition of the encryption key.
SOLUTION: A server 100 and plural clients 200 are connected via a network and the client 200 generates a public key and a private key of an open key encryption in pairs. In the case of generating the keys, the private key is forcibly or automatically deposited. The server 100 holds decoded information encrypted by the public key of a deposit destination and decodes an object private key in cooperation with the deposit destination based on a request of the deposit destination and allows the deposit destination to use the decoded private key.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2000－151574
（P2000－151574A）
(43)公開日　平成12年５月30日(2000.5.30)

(51)Int.Cl.'	識別記号	Ｆ Ｉ		テーマコード'（参考）
Ｈ０４Ｌ　9/08		Ｈ０４Ｌ　9/00	６０１Ｚ	５Ｂ０８９
Ｇ０６Ｆ　13/00	３５１	Ｇ０６Ｆ　13/00	３５１Ｚ	５Ｊ１０４
Ｇ０９Ｃ　1/00	６３０	Ｇ０９Ｃ　1/00	６３０Ｚ	９Ａ００１
			６３０Ｆ	
		Ｈ０４Ｌ　9/00	６０１Ａ	

審査請求　未請求　請求項の数13　ＯＬ　（全 14 頁）　最終頁に続く

(21)出願番号　特願平10－321867

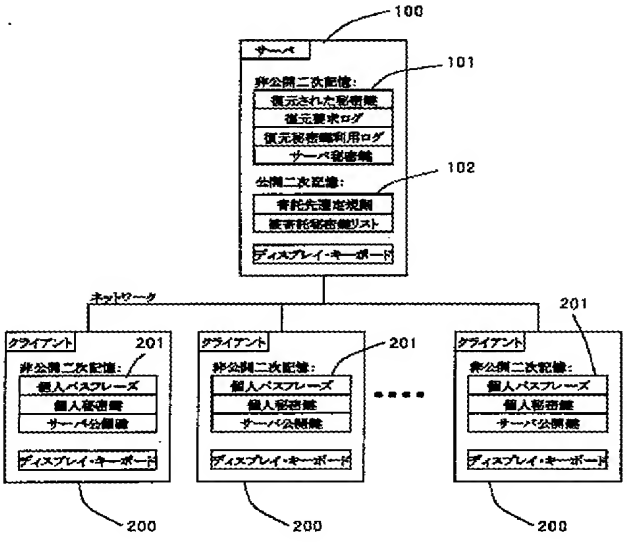
(22)出願日　平成10年11月12日(1998.11.12)

(71)出願人　000005496
富士ゼロックス株式会社
東京都港区赤坂二丁目17番22号
(72)発明者　青木　隆一
神奈川県川崎市高津区坂戸３丁目２番１号
ＫＳＰ　Ｒ＆Ｄ　ビジネスパークビル
富士ゼロックス株式会社内
(74)代理人　100086531
弁理士　澤田　俊夫

Ｆターム(参考)　5B089 GA11 GA21 JB22 KA17 KB13
5J104 AA16 EA12 EA19 JA21 PA07
9A001 CZ08 EE03 JJ27 LL03

(54)【発明の名称】　暗号鍵寄託装置および方法

(57)【要約】
【課題】　秘密鍵の寄託を確実に行なう。
【解決手段】　サーバ１００、複数のクライアント２００がネットワーク３００を介して接続され、クライアント２００は公開鍵暗号の公開鍵および秘密鍵のペアを生成する。この生成時には、秘密鍵が強制的または自動的に寄託される。サーバ１００は、寄託先の公開鍵で暗号化された復元情報を保持し、寄託先の要求に基づいて寄託先と協同して対象秘密鍵の復元を行い、また復元された秘密鍵を寄託先が利用できるようにする。



1

【特許請求の範囲】

【請求項１】　ユーザに対して暗号鍵を生成する手段と、

上記暗号鍵の生成に応答して、上記暗号鍵を、所定の寄託者が上記暗号鍵を復元可能な態様で保管する処理を起動する手段とを有することを特徴とする暗号鍵寄託装置。

【請求項２】　上記暗号鍵は公開鍵暗号方式の秘密鍵とする請求項１記載の暗号鍵寄託装置。

【請求項３】　上記所定の寄託者を決定する規則を設定し、この規則に基づいて上記暗号鍵を保管する請求項１または２記載の暗号鍵寄託装置。

【請求項４】　サーバおよびクライアントを有し、上記暗号鍵を復元するための復元情報が上記寄託先の公開鍵で暗号化されて上記サーバに保持される請求項１、２または３記載の暗号鍵寄託装置。

【請求項５】　上記サーバが、上記寄託者からの復元要求に基づいて、上記寄託先の公開鍵で暗号化された復元情報を上記寄託先へ送付し、上記寄託先で上記寄託先の秘密鍵で復号されたのち、上記サーバの公開鍵で暗号化された復元情報を、上記寄託先から取得し、取得した暗号化復元情報を上記サーバの秘密鍵で復号し、復号した復元情報を用いて寄託対象の上記サーバの秘密鍵で上記暗号鍵の復元情報を復号し、復号した復元情報を用いて上記暗号鍵を復元する請求項４記載の暗号鍵寄託装置。

【請求項６】　上記サーバは上記復元要求に関する履歴を記録する請求項５記載の暗号鍵寄託装置。

【請求項７】　上記サーバが、上記寄託者からの暗号鍵獲得要求に基づいて、上記復元した暗号鍵を上記寄託先の公開鍵で暗号化して上記寄託先に送付する請求項５または６記載の暗号鍵寄託装置。

【請求項８】　上記サーバは上記暗号鍵取得要求に関する履歴を記録する請求項７記載の暗号鍵寄託装置。

【請求項９】　上記サーバは、上記寄託先への復元された暗号鍵の送付を行なわず、上記委託先からの処理要求の基づいて、上記暗号鍵を用いた処理を上記委託先にかわって実行する請求項５または６記載の暗号鍵寄託装置。

【請求項１０】　上記サーバは、上記委託先からの処理要求の履歴を記録する請求項９記載の暗号鍵寄託装置。

【請求項１１】　上記暗号が割り当てられたユーザに上記履歴を供給する請求項６、８または１０記載の暗号鍵寄託装置。

【請求項１２】　ユーザに対して暗号鍵を生成するステップと、

上記暗号鍵の生成に応答して、上記暗号鍵を、所定の寄託者が上記暗号鍵を復元可能な態様で保管する処理を起動するステップとを有することを特徴とする暗号鍵寄託方法。

【請求項１３】　ユーザに対して暗号鍵を生成するステップと、

2

上記暗号鍵の生成に応答して、上記暗号鍵を、所定の寄託者が上記暗号鍵を復元可能な態様で保管する処理を起動するステップとをコンピュータ・システムに実行させるために用いられる暗号鍵寄託用コンピュータ・プログラム製品。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、暗号鍵例えば公開鍵暗号方式の秘密鍵を寄託する技術に関する。

【０００２】

【従来の技術】公開鍵暗号方式を用いて情報を暗号化することにより、情報の機密性を維持することができるが、秘密鍵を利用できないとき、情報の復号が不可能となってしまう。個人を単位とする一般的なセキュリテイでは、その個人がシステムにアクセスできない状況にある（外出、病気、死亡などによる）とき、その個人は秘密鍵が利用できない。そのため、その秘密鍵によって復号可能な情報を復号できない。しかし、そもそも、その個人はシステムにアクセスできないわけであるから、情報にもアクセスできない。そのため秘密鍵が利用できないこと自体は、その個人にとって問題とならない。また、他者がその情報にアクセスしたくとも、その情報は秘密鍵の所有者である個人に属する情報であるから、他者がアクセスできるようにする必要はない。

【０００３】他方、企業向けセキュリティにおいては、秘密鍵が利用できないと問題が生じる。すなわち、企業内の個人は、企業活動の中における役割を果たすために存在している。よって、企業活動上の情報が所定の個人の秘密鍵で暗号化されていたとしても、その情報は企業として必要な情報である。そのため、その個人が外出、病気、死亡などにより、その情報が復号できない場合には、企業内の適切な代理者がその情報にアクセスすることにより、企業活動に支障が生じないようにする必要がある。

【０００４】従来、秘密鍵を寄託する機構は存在したが次のような問題があった。

①寄託の実施は秘密鍵の所有者の自主性に任されていた。もちろん、秘密鍵の寄託を実施しなければならない、というような規則を定めることはできるが、それを遵守することをシステムに保証する方法は存在しなかったし、寄託された秘密鍵が正当なものであることを確認する方法も存在しなかった。

②寄託先の選定が秘密鍵の所有者の判断に任されていた。有効な寄託先に寄託しなければ、万一のときに寄託の効果を得られないし、逆に悪意のある寄託先に寄託することは悪用の危険がある。

③寄託の操作が煩雑であった。一般にフロッピーディスクなどの可搬記憶媒体を用い、複数の可搬記憶媒体に元の秘密鍵を分割して保管し、それぞれを複数の寄託先に

預けるとしう方式を採用するが、その操作は元の所有者にとっても、寄託先にとっても煩雑である。

④寄託先による被寄託秘密鍵の部分の管理が、寄託先に任されている。そのため、寄託先の管理が不十分だと第三者に悪用される可能性ある。

⑤寄託時に指定された人数の寄託者が協調（結託）すれば秘密鍵は復元でき、それを利用可能である。そして、復元および利用の事実は、元の秘密鍵の所有者には知られることはない。よって、悪用が可能である。そのため、秘密鍵の本来の所有者の権利が、犯される可能性があるし、電子署名の信頼性は下がることとなる。

⑥秘密鍵が一度復元されてしまうと、永久に完全に元の秘密鍵の所有者と同一の権利を得ることができる。そのため、秘密鍵の本来の所有者の権利が、犯される可能性があるし、電子署名の信預性は下がることとなる。

【０００５】

【発明が解決する課題】この発明は、以上の事情を考慮してなされたものであり、暗号鍵の寄託をコントロールするスキームを提供し、規則正しく暗号鍵の寄託を実現し、また寄託された暗号鍵のセキュリティを十分に維持できるようにすることを目的としている。

【０００６】

【課題を解決するための手段】本発明においては、次のように暗号鍵例えば秘密鍵の寄託を行う。

（１）秘密鍵の寄託を、秘密鍵と公開鍵のペアを生成すると同時に自動的に実施する機構を設ける。

（２）秘密鍵の寄託先の選定規則を設けて、その規則に基づき寄託先を自動的に選定する。

（３）寄託された鍵の管理行う機構を設け、寄託先の秘密鍵により被寄託秘密鍵を守る。

（４）必要な寄託先が協調しても、元の秘密鍵が得られるのではなく、元の秘密鍵が必要な処理を行えるだけとする。

（５）元の秘密鍵が必要な処理を行える期間に制限を設ける。

（６）元の秘密鍵が必要な処理を秘密鍵を用いた情報の復号のみとする。

【０００７】すなわち、本発明によれば、上述の目的を達成するために、暗号鍵寄託装置に、ユーザに対して暗号鍵を生成する手段と、上記暗号鍵の生成に応答して、上記暗号鍵を、所定の寄託者が上記暗号鍵を復元可能な態様で保管する処理を起動する手段とを設けるようにしている。

【０００８】この構成においては、暗号鍵の寄託をコントロールできるので、システム要求に合致した態様で暗号鍵を寄託でき、また、暗号鍵のセキュリティを十分に維持できる。もちろん、すべての暗号鍵を寄託するのでなく一部のクラスの暗号鍵の寄託をコントロールするようにしてもよい。上記暗号鍵は、例えば、公開鍵暗号方式の秘密鍵である。もちろん慣用暗号鍵方式の暗号鍵を

寄託するようにしてもよい。

【０００９】この構成においては、上記所定の寄託者を決定する規則を設定し、この規則に基づいて上記暗号鍵を保管するようにしてもよい。

【００１０】また、クライアント・サーバ・システムにおいて実現する場合には、上記暗号鍵を復元するための復元情報が上記寄託先の公開鍵で暗号化されて上記サーバに保持されるようにしてもよい。この場合、上記サーバが、上記寄託者からの復元要求に基づいて、上記寄託先の公開鍵で暗号化された復元情報を上記寄託先へ送付し、上記寄託先で上記寄託先の秘密鍵で復号されたのち、上記サーバの公開鍵で暗号化された復元情報を、上記寄託先から取得し、取得した暗号化復元情報を上記サーバの秘密鍵で復号し、復号した復元情報を用いて寄託対象の上記サーバの秘密鍵で上記暗号鍵の復元情報を復号し、復号した復元情報を用いて上記暗号鍵を復元するようにしてもよい。そして、上記サーバは上記復元要求に関する履歴を記録するようにしてもよい。

【００１１】また、上記サーバが、上記寄託者からの暗号鍵獲得要求に基づいて、上記復元した暗号鍵を上記寄託先の公開鍵で暗号化して上記寄託先に送付するようにしてもよい。そして、上記サーバは上記暗号鍵取得要求に関する履歴を記録するようにしてもよい。

【００１２】また、上記サーバは、上記寄託先への復元された暗号鍵の送付を行なわず、上記委託先からの処理要求の基づいて、上記暗号鍵を用いた処理を上記委託先にかわって実行するようにしてもよい。そして、上記サーバは、上記委託先からの処理要求の履歴を記録するようにしてもよい。

【００１３】上記履歴は、暗号所有者に送られる。

【００１４】なお、本発明は、方法としても、コンピュータ・プログラム製品としても実現可能であることはもちろんである。

【００１５】

【発明の実施の態様】以下、本発明を詳細に説明する。

（１）秘密鍵の寄託先選定（グループ階層の利用）

秘密鍵の自動寄託関連において、以下では暗号技術を用いて、正当でない要求への応答を防ぐことにしている。しかし、暗号技術を用いない方法もありえる。

【００１６】第一の処理は、寄託先の選定である。寄託先とは、被寄託個人秘密鍵を預ける先を意味する。正確には、被寄託個人秘密鍵を取得、もしくは利用する権利を持つ個人もしくはグループ（今までと同様にグループには役割を含む）である。グループが指定された場合には、そのグループの任意のメンバが被寄託個人秘密鍵の取得もしくは利用の権利を有することとなる。

【００１７】寄託先の選定方法には、例えばつぎのものである。

①グループ階層全体としての寄託先選定規則を指定し、それに従う。例えば、「直属のグループの責任者と、さ

5

らにその直上のグループの責任者の一つ」、「直属のグループの責任者と、直属のグループ」、といったものである。

②個々のグループとしての寄託先選定規則を指定する。

③被寄託個人秘密鍵の所有者が指定する。

【００１８】複数の寄託先を指定した場合には、そのうち幾つの寄託先の指示に従い、被寄託個人秘密鍵に関する権利が利用可能となるかどうかを指定する。ここで指定した数を必要寄託先数と呼ぶ。

【００１９】（２）秘密鍵の寄託先選定（申告制）

寄託先の指定方法としてグループ階層を用いない方法もある。すなわち、各個人が自由に、もしくは何らかの運用規則に従って寄託先を指定し、それを他者に知らせ、許可を受ける、もしくは他者に知らせ寄託先指定に関する検査を可能とする。必要寄託先数などの指定はグループ階層を利用した場合と同様である。

【００２０】（３）秘密鍵自動寄託

被寄託個人秘密鍵を、寄託先に対応した公開鍵で暗号化し、サービスなどに保管する。必要寄託先数が２以上の場合には、被寄託個人秘密鍵を分割して、各公開鍵で暗号化する。この分割方法などについては既に知られている方式を用いる。既に知られている分割方法は、例えば、寄託先が３、必要寄託先数が２の場合には、元の秘密鍵を３等分し（３等分されたものをそれぞれＸｐ１、Ｘｐ２、Ｘｐ３と呼ぶことにする）、Ｘｐ１＋Ｘｐ２、Ｘｐ１＋Ｘｐ３、Ｘ２＋Ｘｐ３の組み合わせを作り、３人の寄託先に分配する。任意の二人の寄託先が持つ組み合わせを持ち寄れば、元の秘密鍵を再構成できる。

【００２１】被寄託個人秘密鍵は、所有者のみが持っているため、所有者のクライアントにおいて、必要に応じて分割し、寄託先に対応した公開鍵で暗号化し、さらにサービスの公開鍵で暗号化し、サービスもしくは寄託先に送る。

【００２２】（４）被寄託秘密鍵の管理

寄託された被寄託秘密鍵は、寄託先の公開鍵で暗号化した形で、寄託先もしくはサービスで管理する。

（５）被寄託秘密鍵取得

寄託先の個人もしくはグループのメンバが、被寄託個人秘密鍵の特定して、その利用を要求する。これにより、保管されている被寄託個人秘密鍵が復号される。この機能を提供する代わりに使用権だけを提供する方法もある。使用権の提供については後述する。

【００２３】保管されている暗号化済み被寄託個人秘密鍵（全体もしくは部分）を必要数だけ集め、元の個人秘密鍵を再構成する。サービス経由方式と、寄託者個人間で行う方式とがある。

【００２４】（６）被寄託秘密鍵利用権取得

これは秘密鍵自体を、寄託者という他者が入手してしまうと、以降自由に利用できてしまうため、個人の秘密鍵の使用者を限定度が疑わしいものとなり、公開鍵暗号方

6

式自体を危うくしてしまう。そのため、寄託者に対して秘密鍵自体を取得させるのではなく、利用だけを可能とするものである。すなわち、再構成した被寄託秘密鍵はサービスの中か、クライアントシステム中にだけに存在することとし、寄託者からの、秘密鍵を用いて可能な復号処理を、サービスが代行する。

【００２５】（７）被寄託秘密鍵利用履歴保存および事後通知

被寄託秘密鍵の利用権をサービスを経由して与える方式を用いる場合には、サービスが代行した処理の履歴をとり、被寄託秘密鍵の所有者に事後通知する。個々の履歴の内容は、要求者、時刻、対象処理（一般には復号のみ）、対象情報である。通知方法は、電子メールが好ましい。また通知先を所有者本人だけでなく、直上のグループの責任者（要するに上司）にも通知することも、不正を防止したり、不用意に被寄託秘密鍵利用権取得を行わないために有効である。

【００２６】

【実施例】以下、本発明の実施例について詳細に説明する。

【００２７】以下の説明においては用語はつぎのような意味を有するものとする。

【００２８】

【表１】

［用語］

・対象秘密鍵：　寄託される秘密鍵

・秘密鍵所有者：　対象秘密鍵の所有者

・寄託先：　対象秘密鍵の寄託先である個人

・被寄託秘密鍵：　実際に寄託先に送られる、対象秘密鍵を再構成するために必要な情報

・寄託先数：　一つの対象秘密鍵の寄託先の数

・必要寄託先数：　対象秘密鍵を再構成するために必要な被寄託秘密鍵の個数

【００２９】図１は、実施例の全体的な構成を示しており、この図において、サーバ１００、複数のクライアント２００がネットワーク３００を介して接続されている。ネットワーク３００は、企業全体のシステムを接続するものであり、ＬＡＮまたはＬＡＮセグメントをＷＡＮで接続してなるものである。サーバ１００およびクライアント２００は通常のコンピュータシステムのリソースを有するものであり、その構成は通常のものと同様であるので説明は行なわない。サーバ１００は非公開二次記憶１０１および公開二次記憶１０２を有している。クライアント２００は非公開二次記憶２０１を有している。非公開二次記憶１０１、２０１中の情報は他からは直接に参照することはできない。公開二次記憶１０２中の情報は他から自由に参照することができる。ただし、他からの変更はできない。

7

【００３０】サーバ１００の非公開二次記憶１０１は、サーバ秘密鍵、復元された秘密鍵、復元要求ログ、復元秘密鍵利用ログ等を保持している。サーバ１００の公開二次記憶１０２は、寄託先選定規則、被寄託秘密鍵リスト等を保持している。クライアント２００の非公開二次記憶２０１は個人パスフレーズ、個人秘密鍵、サーバ公開鍵等を保持している。

【００３１】図に示す例では、被寄託秘密鍵の管理や、秘密鍵の復元処理、ログの記録はサーバ１００で行う構成としている。ただし、これらをクライアント２００のみで行うことも可能である。

【００３２】つぎに実施例の動作について説明する。

（１）「秘密鍵寄託規則の設定」（図２）

この処理は、各個人を統括する役割を持つ個人が、その個人のクライアント２００において行う処理である。設定された規則にしたがって寄託先がコントロールされる。なお、「秘密鍵寄託箱則の設定」を行なって規則にしたがった寄託先の決定を行なう代りに、「秘密鍵寄託先の自主的な設定（１）」（図３）や「秘密鍵寄託先の自主的な設定（２）」（図４）の手法を行なって寄託先を決定するようにしてもよい。どの手法を採用するかはシステムの要請に依存する。

【００３３】秘密鍵寄託規則の設定」の処理は以下のように行なわれる。

［ステップＳ１１］：直属グループ責任者、直属のさらに直属グループ責任者、同一グループの他のメンバの３つのタイプから１つ以上を選ぶ。

［ステップＳ１２］：必要寄託先数（１以上で所定数以下）を指定する。

【００３４】寄託先は以上の規則にしたがって行われる。必要であればユーザが補助的な選択を行なう。

【００３５】（２）「秘密鍵寄託先の自主的な設定（１）」（図３）

この処理は、各個人が自身のクライアント２００において行う処理である。この方式を選択した場合には、図１中のサーバ１００に「寄託先選定規則」を保持する必要がなくなり、代わりに、所定のＣＡ（公証局）に、公開鍵に対応して、寄託先を示す項目を追加する必要がある。ＣＡは図１中に描かれていないが、公開鍵暗号方式を用いる場合には、一般的に存在するサービスである。

【００３６】「秘密鍵寄託先の自主的な設定（１）」の処理は次のように行なわれる。

［ステップＳ２１］：寄託先である一人以上の個人と、必要寄託先数とを指定する。

［ステップＳ２２］：ＣＡに指定された情報を自動的に送付し、公開鍵と対応づける。

【００３７】（３）「秘密鍵寄託先の自主的な設定（２）」（図４）

この処理は、各個人が自身のクライアント２００において行う処理である。この方式を選択した場合には、図１

8

中でサーバ１００は「寄託先選定規則」を保持する必要がなく、代わりに、各クライアント２００に、報告者が寄託先が適正であることを承認したことを示す情報を格納する領域（図示しない）が必要となる。

【００３８】「秘密鍵寄託先の自主的な設定（２）」の処理は次のように行なわれる。

［ステップＳ３１］：寄託先の報告先を指定する。

［ステップＳ３２］：寄託先である一人以上の個人と、必要寄託先数を指定する。

［ステップＳ３３］：指定された情報を報告先に自動的に送付する。

［ステップＳ３４］：報告先で送付された情報を評価する。

［ステップＳ３５］：評価結果が適正であったならば、適正であることを送付元の個人のクライアント２００に伝達する。

［ステップＳ３６］：適正である場合に限り、公開鍵と秘密鍵のペアを生成可能にする。

【００３９】（４）「秘密鍵の自動寄託」（図５）

この処理は、各クライアント２００において公開鍵と秘密鍵のペアを生成した際に、引き続いて行われる処理である。この処理に先立って、「秘密鍵寄託規則の設定」（図２）、「秘密鍵寄託先の自主的な設定（１）」（図３）、「秘密鍵寄託先の自主的な設定（２）」（図４）のうちいずれか一つが実施されている必要がある。

【００４０】「秘密鍵の自動寄託」の処理は次のように行なわれる。

［ステップＳ４１］：公開鍵と秘密鍵のペアを生成する。

［ステップＳ４２］：寄託先数と必要寄託数より、寄託先数の個数の被寄託秘密鍵を生成する。

［ステップＳ４３］：寄託先の公開鍵で被寄託秘密鍵を暗号化する。

［ステップＳ４４］：サーバ１００に暗号化された被寄託秘密鍵を送付する。

［ステップＳ４５］：サーバ１００において、暗号化された被寄託秘密鍵を記録する。

【００４１】（５）「秘密鍵復元」（図６）

この処理は、必要寄託先数の数の寄託先である個人が各クライアント２００において行う処理である。「秘密鍵復元」の処理は次のように行なわれる。

［ステップＳ５１］：協調が必要な寄託先数となるまで、ステップＳ５７までの処理を繰り返す。

［ステップＳ５２］：クライアント２００は、秘密鍵所有者と自身をサーバ１００に提示する。

［ステップＳ５３］：サーバ１００は、秘密鍵利用権取得要求の要求元と秘密鍵所有者の復元要求のログを記録する。

［ステップＳ５４］：サーバ１００は、被寄託秘密鍵を返す。

［ステップＳ５５］：クライアント２００は自身の秘密鍵により、返された被寄託秘密鍵を復号する。

［ステップＳ５６］：クライアント２００は、復号した被寄託秘密鍵をサーバ１００の公開鍵で暗号化する。

［ステップＳ５７］：サーバ１００の公開鍵で暗号化した被寄託秘密鍵をサーバ１００に返す。

［ステップＳ５８］：協調が必要な寄託先数になったらステップＳ５９に進む。

［ステップＳ５９］：サーバ１００が、寄託先の各々から送られてきた、サーバ１００の公開鍵で暗号化された被寄託秘密鍵を、サーバ１００の秘密鍵で復号する。

［ステップＳ６０］：サーバ１００が、復号した被寄託秘密鍵を合成して元の秘密鍵を復元する。

［ステップＳ６１］：サーバ１００は、秘密鍵を復元した時刻を記憶する。

［ステップＳ６２］：復元した時刻から所定時間経過したかどうかを逐次判別し、経過したらステップＳ６３に進む。

［ステップＳ６３］：タイムアップに応じて秘密鍵を削除する。

【００４２】（６）「秘密鍵獲得」（図７）

この処理は、寄託先である個人が復元された秘密鍵自体を獲得する処理である。この処理を提供せず、「秘密鍵利用」（図８）のみを提供する方が、秘密鍵の不正利用を防ぎ、秘密鍵の信頼性を維持する効果がある。

【００４３】「秘密鍵獲得」の処理は次のように行なわれる。

［ステップＳ７１］：クライアント２００において、秘密鍵所有者と自身とをサーバ１００に提示する。

［ステップＳ７２］：サーバ１００は、対象秘密鍵がすでに復元されてサーバに存在するかどうかを判別する。存在しなければ処理を終了する。存在すればステップＳ７３に進む。

［ステップＳ７３］：サーバ１００は、対象秘密鍵の復元要求元のログに獲得要求者が含まれるかどうかを判別し、含まれないならば、処理を終了し、含まれていれば、ステップＳ７４へ進む。

［ステップＳ７４］：サーバ１００は、対象秘密鍵を要求者の公開鍵で暗号化する。

［ステップＳ７５］：サーバ１００は、暗号化した対象秘密鍵を要求者に送付する。

［ステップＳ７６］：クライアント２００において、送付されてきた、暗号化された対象秘密鍵を要求者の秘密鍵で復号する。

【００４４】（７）「秘密鍵利用」（図８）

この処理は、寄託先である個人が秘密鍵を利用する処理である。ここでは当該秘密鍵でのみ復号可能な情報の復号だけを提供する例を示している。

【００４５】「秘密鍵利用」の処理は次のように行なわれる。

［ステップＳ８１］：クライアント２００において、サーバ１００に、秘密鍵所有者と自身を提示する。

［ステップＳ８２］：サーバ１００は、対象秘密鍵がすでに復元されていてサーバ１００に存在するかどうかを判別し、存在していなければ処理を終了し、存在していればステップＳ８３に進む。

［ステップＳ８３］：サーバ１００は、対象秘密鍵の復元要求元のログに獲得要求者が含まれるかどうかを判別し、含まれないならば、処理を終了し、含まれていれば、ステップＳ８４へ進む。

［ステップＳ８４］：サーバ１００は、要求者が復号したい暗号化済み情報を要求者から受け取る。

［ステップＳ８５］：サーバ１００は、復号要求に関連して、対象情報、日時、要求者、秘密鍵所有者を復元秘密鍵利用ログに記録する。

［ステップＳ８６］：サーバ１００は、暗号化済み情報を、復元された秘密鍵で復号する。

［ステップＳ８７］：サーバ１００は、復号された情報を、要求者の公開鍵で暗号化する。

［ステップＳ８８］：サーバ１００は、暗号化された情報を要求者に送付する。

［ステップＳ８９］：クライアント２００において、要求者はサーバからの情報を自身の秘密鍵で復号する。

【００４６】（８）「秘密鍵利用記録の提示」（図９）

この処理は、秘密鍵の所有者に対して、秘密鍵の復元や利用などについて、事後報告する処理であり、秘密鍵の所有者が任意の目的でサーバ１００にアクセスしたときに、自動的に行われる処理である。

【００４７】「秘密鍵利用記録の提示」の処理は次のように行なわれる。

［ステップＳ９１］：クライアント２００において、秘密鍵所有者がサーバ１００にアクセスする。

［ステップＳ９２］：サーバ１００は、アクセスした秘密鍵所有者に関連して、復元要求ログ、復元秘密鍵利用ログがあるかどうかを判別し、なければ処理を終了し、あればステップＳ９３へ進む。

［ステップＳ９３］：サーバ１００は、元要求ログ、復元秘密鍵利用ログを秘密鍵所有者に送付する。

【００４８】

【発明の効果】以上説明したように、この発明によれば、暗号鍵の寄託をコントロールするスキームを採用して、規則正しく暗号鍵の寄託を実現し、また寄託された暗号鍵のセキュリティを十分に維持できる。

【図面の簡単な説明】

【図１】　本発明の実施例の構成を全体として示すブロック図である。

【図２】　上述実施例の「秘密鍵寄託規則の設定」処理を説明するフローチャートである。

【図３】　上述実施例の「秘密鍵寄託先の自主的な設定（１）」処理を説明するフローチャートである。

【図４】　上述実施例の「秘密鍵寄託先の自主的な設定（２）」処理を説明するフローチャートである。

【図５】　上述実施例の「秘密鍵の自動寄託」処理を説明するフローチャートである。

【図６】　上述実施例の「秘密鍵復元」処理を説明するフローチャートである。

【図７】　上述実施例の「秘密鍵獲得」処理を説明するフローチャートである。

【図８】　上述実施例の「秘密鍵利用」処理を説明するフローチャートである。

【図９】　上述実施例の「秘密鍵利用記録の提示」処理を説明するフローチャートである。

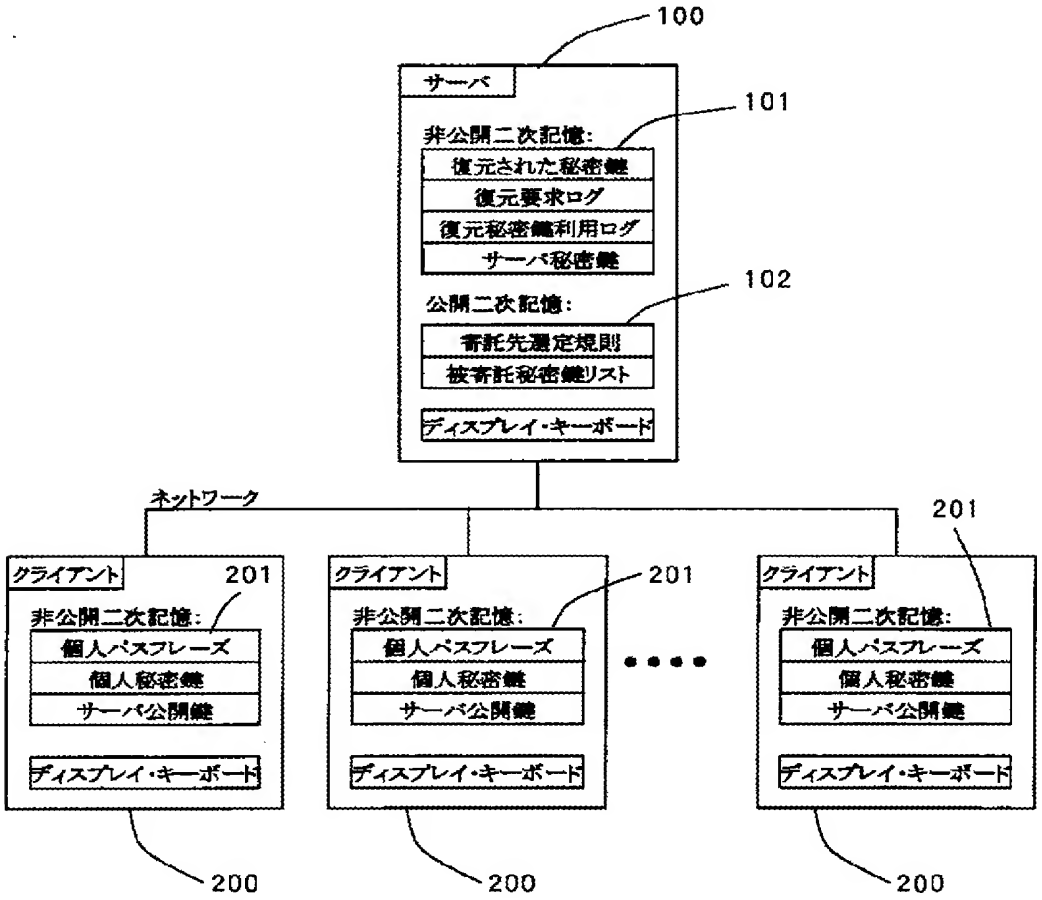
【符号の説明】

１００　　サーバ

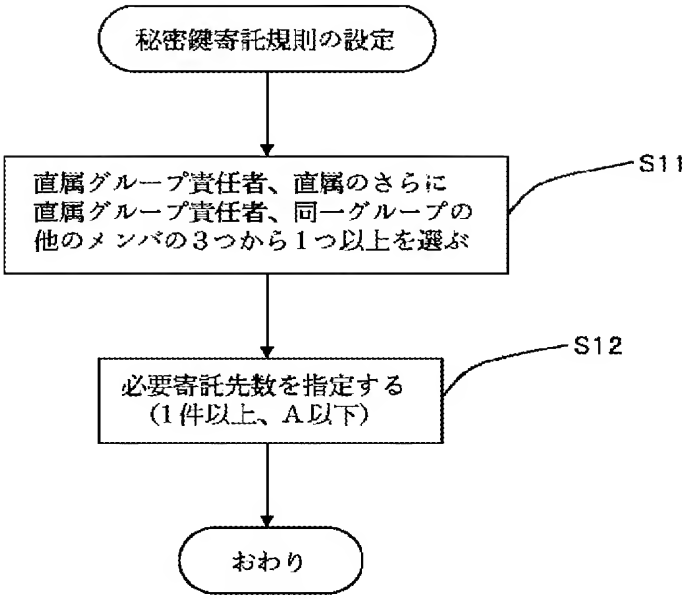
２００　　クライアント

３００　　ネットワーク

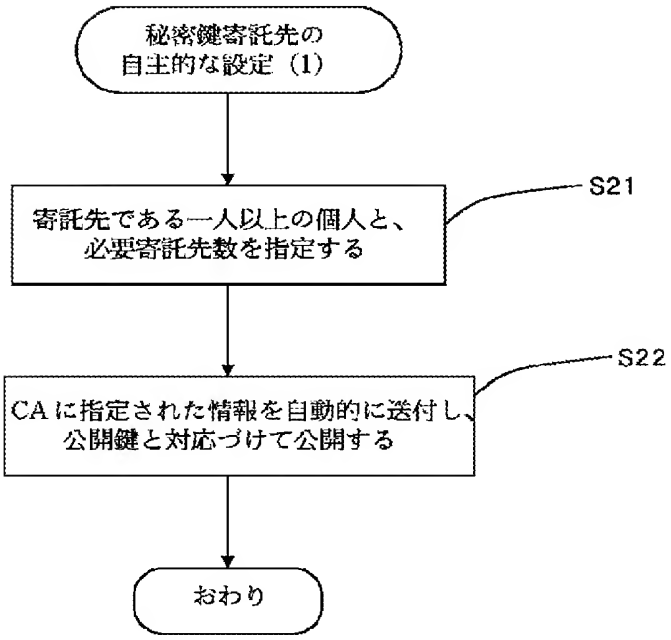
【図１】



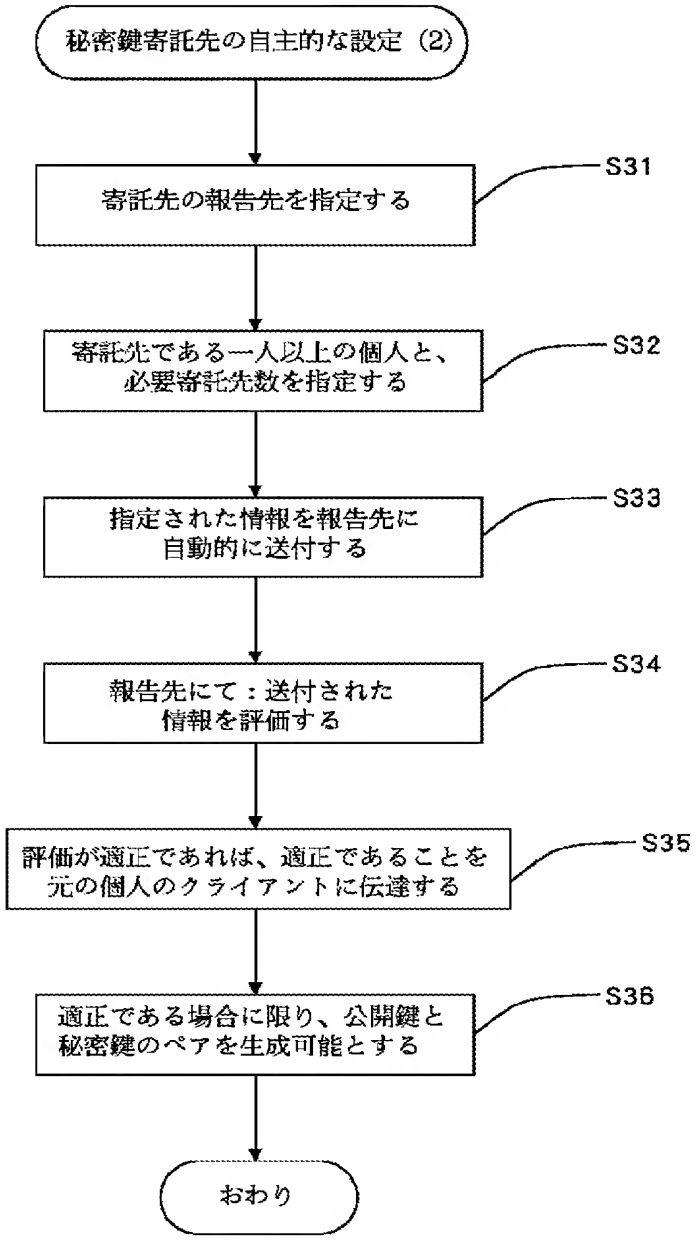
【図２】


秘密鍵寄託規則の設定
直属グループ責任者、直属のさらに
直属グループ責任者、同一グループの
他のメンバの３つから１つ以上を選ぶ
S11
必要寄託先数を指定する
（1件以上、A以下）
S12
おわり

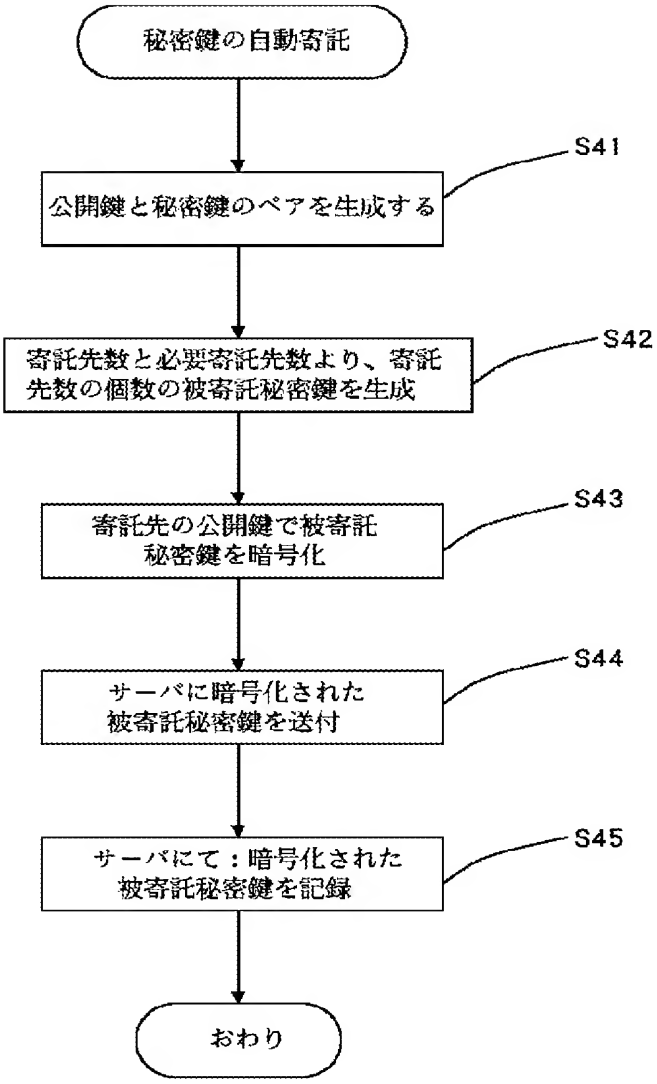
【図３】


秘密鍵寄託先の
自主的な設定（1）
寄託先である一人以上の個人と、
必要寄託先数を指定する
S21
CAに指定された情報を自動的に送付し、
公開鍵と対応づけて公開する
S22
おわり

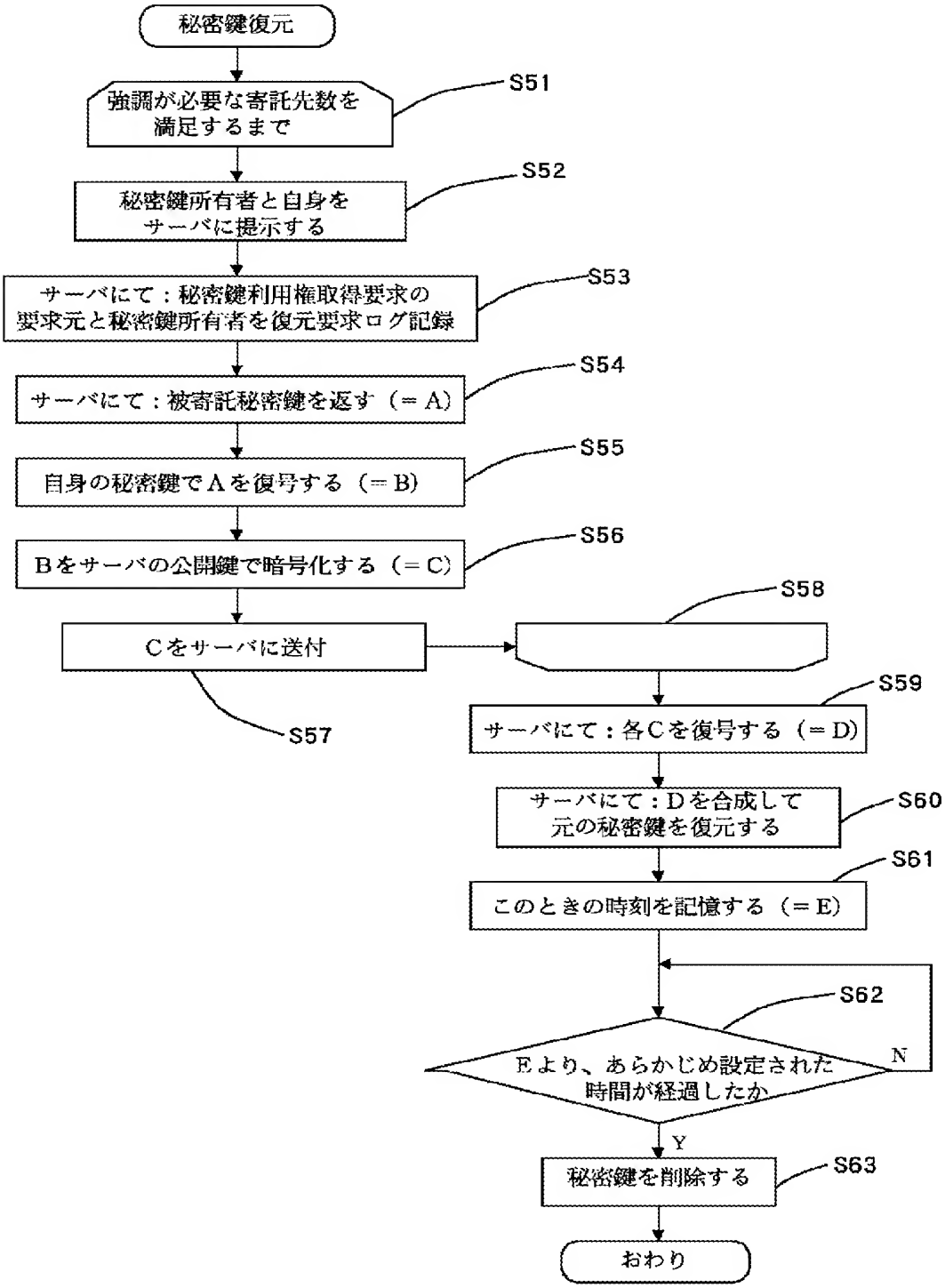
【図４】


秘密鍵寄託先の自主的な設定（2）
寄託先の報告先を指定する
S31
寄託先である一人以上の個人と、
必要寄託先数を指定する
S32
指定された情報を報告先に
自動的に送付する
S33
報告先にて：送付された
情報を評価する
S34
評価が適正であれば、適正であることを
元の個人のクライアントに伝達する
S35
適正である場合に限り、公開鍵と
秘密鍵のペアを生成可能とする
S36
おわり

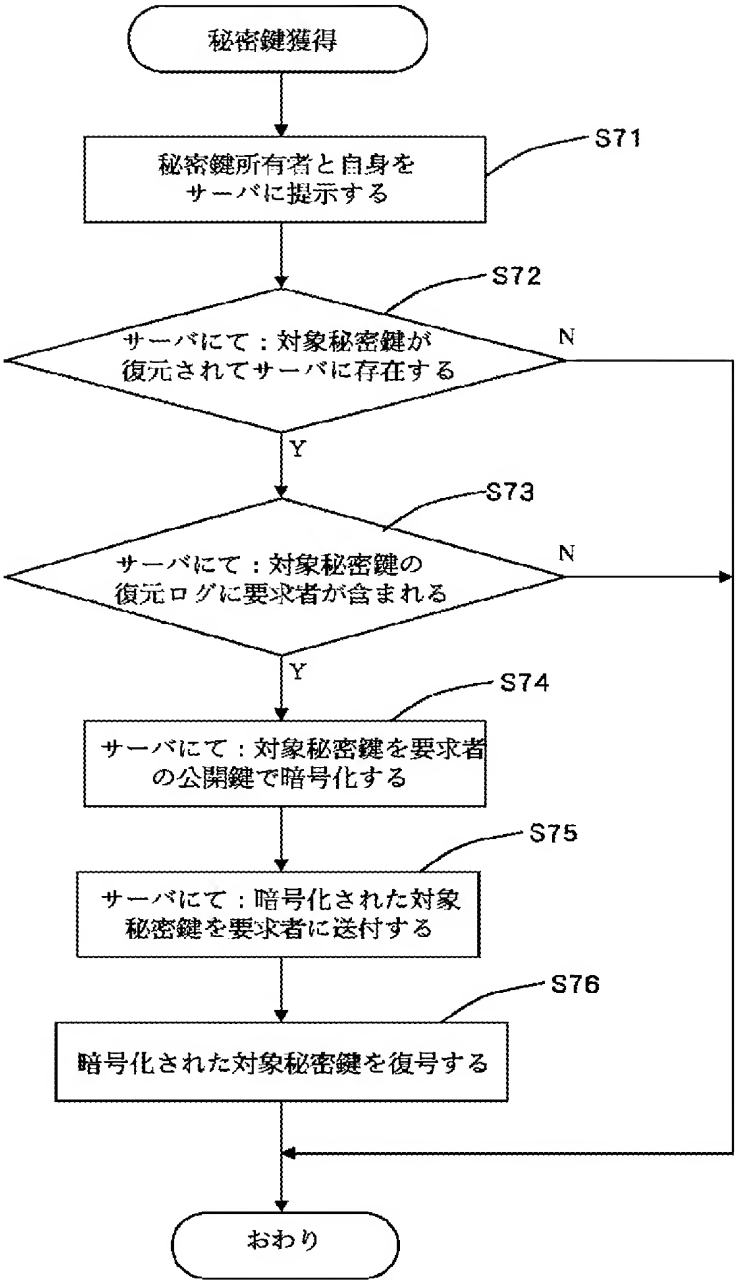
【図５】


秘密鍵の自動寄託
S41
公開鍵と秘密鍵のペアを生成する
S42
寄託先数と必要寄託先数より、寄託先数の個数の被寄託秘密鍵を生成
S43
寄託先の公開鍵で被寄託秘密鍵を暗号化
S44
サーバに暗号化された被寄託秘密鍵を送付
S45
サーバにて：暗号化された被寄託秘密鍵を記録
おわり

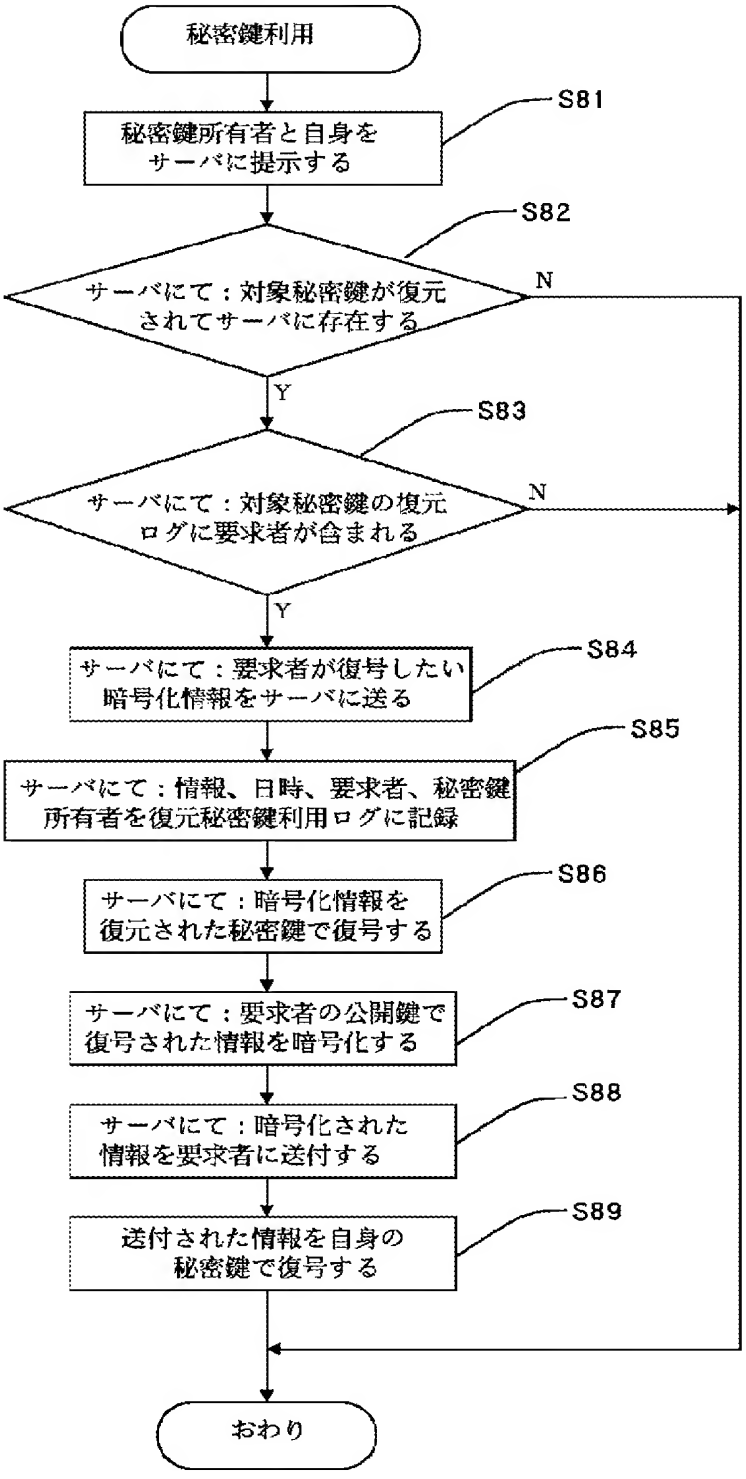
【図６】


秘密鍵復元
強調が必要な寄託先数を満足するまで
S51
秘密鍵所有者と自身をサーバに提示する
S52
サーバにて：秘密鍵利用権取得要求の要求元と秘密鍵所有者を復元要求ログ記録
S53
サーバにて：被寄託秘密鍵を返す（＝A）
S54
自身の秘密鍵でAを復号する（＝B）
S55
Bをサーバの公開鍵で暗号化する（＝C）
S56
Cをサーバに送付
S57
S58
サーバにて：各Cを復号する（＝D）
S59
サーバにて：Dを合成して元の秘密鍵を復元する
S60
このときの時刻を記憶する（＝E）
S61
Eより、あらかじめ設定された時間が経過したか
S62
N
Y
秘密鍵を削除する
S63
おわり

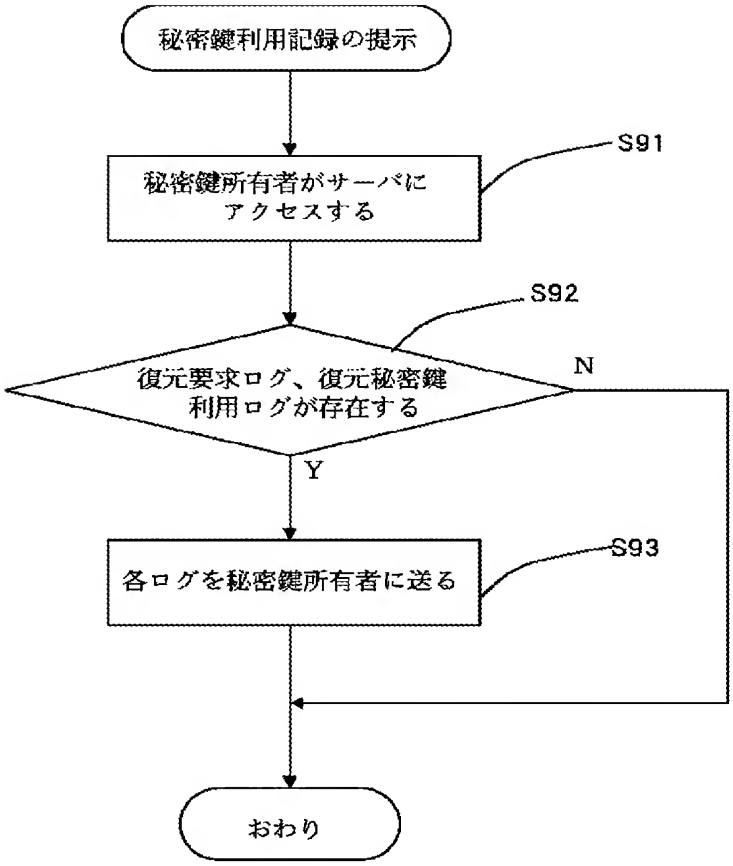
【図７】


秘密鍵獲得
秘密鍵所有者と自身を
サーバに提示する
S71
S72
サーバにて：対象秘密鍵が
復元されてサーバに存在する
N
Y
S73
サーバにて：対象秘密鍵の
復元ログに要求者が含まれる
N
Y
S74
サーバにて：対象秘密鍵を要求者
の公開鍵で暗号化する
S75
サーバにて：暗号化された対象
秘密鍵を要求者に送付する
S76
暗号化された対象秘密鍵を復号する
おわり

【図８】


秘密鍵利用
S81
秘密鍵所有者と自身を
サーバに提示する
S82
サーバにて：対象秘密鍵が復元
されてサーバに存在する
N
Y
S83
サーバにて：対象秘密鍵の復元
ログに要求者が含まれる
N
Y
S84
サーバにて：要求者が復号したい
暗号化情報をサーバに送る
S85
サーバにて：情報、日時、要求者、秘密鍵
所有者を復元秘密鍵利用ログに記録
S86
サーバにて：暗号化情報を
復元された秘密鍵で復号する
S87
サーバにて：要求者の公開鍵で
復号された情報を暗号化する
S88
サーバにて：暗号化された
情報を要求者に送付する
S89
送付された情報を自身の
秘密鍵で復号する
おわり

【図９】



フロントページの続き

(51) Int. Cl.[7]	識別記号	ＦＩ		ﾃｰﾏｺｰﾄﾞ（参考）
		Ｈ０４Ｌ	9/00	６０１Ｆ